Tu

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/622,722	07/18/2003	Hidema Tanaka	43521-0700	2951

21611 7590 01/18/2007
SNELL & WILMER LLP
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/622,722	**Applicant(s)** TANAKA ET AL.
	Examiner Chinwendu C. Okoronkwo	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 January 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *20040629*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-4 are presented for examination.

2. Claims 1-4 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 are rejected under 35 U.S.C. 102(b) as being disclosed by Tsunoo et al. (European Patent Application Publication 0932272 A2).

Regarding claim 1, Tsunoo et al., discloses a cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption, the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein: the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round; the session key prospect calculating section is operative to: calculate one session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation; the untransformed text calculating unit body is operative to: calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; and repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect (0017-0021, 0037-0043 and 0079-0119).

Regarding claim 2, Tsunoo et al., discloses a cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption, the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein: the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round; the session key prospect calculating section is operative to: dynamically create a condition for use in calculating one session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate the session key prospect based on the condition thus created or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation; the untransformed text calculating unit body is operative to: calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect (0017-0021, 0037-0043 and 0079-0119).

Regarding claim 3, Tsunoo et al., discloses a cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption, the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein: the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round; the session key prospect calculating section is operative to: dynamically create conditions for use in calculating a session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate the session key prospect based on the conditions thus created or identify inability to calculate when inconsistency is found between certain two of the conditions and then output uncalculability identifier data indicative of inability to calculate; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation; the untransformed text calculating unit body is operative to calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect (0017-0021, 0037-0043 and 0079-0119).

Regarding claim 4, Tsunoo et al., discloses a cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption, the cipher strength estimating device comprising a first untransformed text calculating unit, a second untransformed text calculating unit, and a control unit, the first untransformed text calculating unit comprising an untransformed text calculating unit body and a first session key prospect calculating section, the second untransformed text calculating unit comprising a second session key prospect calculating section, wherein: the first untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round; the second untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round; the first session key prospect calculating section is operative to: conduct brute-force search for the session key to be used at a certain round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate one session key prospect presumed to be equivalent to the session key to be used at said certain round of transformation or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for said certain round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation; the second session key prospect calculating section is operative to: dynamically create plural conditions for use in calculating a session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by higher order differential cryptanalysis using the plaintext and one of the ciphertext and the putative transformed text; and calculate one session key prospect based on the conditions thus created or identify inability to calculate when inconsistency is found between certain two of the conditions and then output uncalculability identifier data indicative of inability to calculate; the untransformed text calculating unit body is operative to calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the first untransformed text calculating unit; receive the putative untransformed text outputted; input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the second untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the first session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the second session key prospect calculating section to cause the first session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect (0017-0021, 0037-0043 and 0079-0119).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CCO

January 6, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/6/07